UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/610,722	07/06/2000	Suresh Krishna	1875.4310002	5437

28393 7590 02/24/2010

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
1100 NEW YORK AVE., N.W.
WASHINGTON, DC 20005

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2433	

MAIL DATE	DELIVERY MODE
02/24/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/610,722	KRISHNA ET AL.	
	Examiner	Art Unit	
	CARL COLIN	2433	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 November 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *46-70* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *46-70* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____ .

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 11/23/2009, the following claims 46-70 are presented for examination.

2. Applicant's arguments, filed on 11/23/2009, see pages 7-13, have been fully considered, but they are not persuasive. With respect to the 112th rejection first paragraph, Applicant argues that the passage stating that key features of ACE include: "*four datagrams can be processed simultaneously and out of order to keep throughput at full rated wirespeed*" fully supports the claim limitation *determining security association information with each data packet in a plurality of data packets associated with a data flow between a source and destination simultaneously.* Examiner respectfully disagrees because the passage does not state that security association information is being determined, it merely mentions datagram processing. Examiner acknowledges that the original specification discusses parallel processing, but nothing in the specification explicitly describes determining security association information with each data packet in a plurality of data packets associated with a data flow between a source and destination simultaneously.

Applicant argues on pages 10-11 that the Examiner equates L2 and L3 flags to security association information. Examiner respectfully disagrees. The rejection does not state that the flags represent security association, but shows that all the header information including the flags

that can be derived from the header information as meeting the claim recitation of security association information. As reproduced herein Oskouy et al discloses,

L3 Header Processing

The next layer **header processing can be performed in parallel** to the data transfers to the cell payload queue. In one implementation, L3 header processing is performed in parallel to the packing of data by cell packetizer 391. L3 header parser 406 snoops on the bus between the cell packetizer and cell payload queue 388 **examining the L3 header data** to derive a header to be stored in an associated entry in cell header queue 390. *(See column 10, lines 41-49)*.

The flags store information required for the efficient down-stream processing of a given packet. In one implementation, the L2 flags derived during L2 processing include a packet loss priority flag, a send packet to processor flag, a sample packet flag and a physical multicast flag. The L3 flags derived during L3 header processing include an option flag, packet priority flag, transmission control protocol (TCP) flag, protocol type flag, and DF (don't fragment) flag.

The option flag indicates that the packet has an option header (indicates that the L3 header is greater than the minimal size, e.g., 20 bytes for IPV4 packets). The packet priority flag indicates the **priority of the packet** and is used by the output portion of the multi-function multiport. The TCP flag **indicates the packet is a TCP packet**. The protocol flag indicates the L3 **protocol type**. The protocol flag is used by the input switch to determine the **length of the key** to be passed to the controller. The DF flag indicates whether the packet is to be fragmented. Fragmentation may occur at the output interface depending on the configuration of the particular interface. Setting the DF flag will result in the dropping of the packet at the output interface rather than fragment. *(See column 11, lines 17-25 and lines 40-53)*.

Packet header field 360 contains **header information associated with a given packet and includes start offset information, packet length, interface index information and L2 and L3 flags generated as part of the L2 and L3 decoding processes recited above**. *(See column 12, lines 50-54)*.

In operation, packets are received at a multi-function multiport 150, transferred to input switch 100 and stored temporarily in global data buffer 104. When the packet is received by input switch 100, **a key is read from the packet** and transferred to controller 106. **The key contains destination information which is derived from a header field associated with the first block of data in a packet and other information (such as source ID, priority data and flow ID)**. *(See column 5, lines 34-41)*.

As shown above, it is clear that Oskouy discloses security association information as interpreted by the Examiner and as interpreted in the light of applicant's specification (see page 11, lines 1-2 disclosing "*where a classification engine rapidly determines* ***security association information*** *required for processing the packet, such as encryption keys,* ***data****, etc.*). Also, on pages 21-22, applicant's original specification shows matching of IP security association information, which includes **IP address, port and protocol** (see also security association table on page 22). Therefore, Applicant has not overcome the rejection of claims 46-70 and they remain rejected in view of the prior art.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 46-70 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant

art that the inventor(s), at the time the application was filed, had possession of the claimed invention. In the original specification, Examiner was not able to find a classification module determining security association information with each data packet in a plurality of data packets associated with a data flow between a source and destination simultaneously. It appears that the claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Examiner is not convinced that "*four datagrams can be processed simultaneously and out of order to keep throughput at full rated wirespeed*" as cited by Applicant fully supports the claim limitation as claimed above as the processing does not equate or inherently involves determining security association information with each data packet in a plurality of data packets associated with a data flow between a source and destination simultaneously. Applicant is kindly requested to indicate where the claims as amended have support in the original specification.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to

which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 46-49, 55-57, 60, and **64-66** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,870,479 to **Feiken et al** in view of US Patent 6,791,947 to **Oskouy et al**.

As per claim 46, **Feiken et al** discloses a device comprising: an identification unit (classification module) in the device that determines security association information associated with a data flow between a source and destination (see column 3, line 65 through column 4, line 5); a plurality of processing units coupled to the identification unit that meets the recitation of a plurality of processing engines coupled to the classification module (see column 3, lines 59-65), each of the plurality of security processing engines configured to receive at least a portion of the security association information associated with a data packet in the plurality of data packets along with the corresponding data packet (see column 4, lines 7-25), wherein at least two of the plurality of security processing engines receive security association information for different packets (see column 4, lines 25-41); wherein the classification module (identification unit) is configured to provide at least a portion of the security association information associated with the data packets to the plurality of security processing engines (see column 3, line 65 through column 4, line 8); wherein the plurality of security processing engines are configured to process a plurality of the data packets in parallel (see column 4, lines 25-41). **Feiken et al** does not explicitly state that the classification module is configured to determine the security association

information associated for the plurality of data packets simultaneously. **Oskouy et al** in an analogous art discloses receiving a plurality of data packets and performed pre-processing in parallel that meets the recitation of determining security association for the plurality of data packets simultaneously (see column 2, lines 2-5 and column 4, lines 24-29), the L3 header pre-processing that occurs in parallel includes examining the packet headers to derive a header to be stored in an associated entry in cell header queue and deriving key length, priority of the packet, whether it is a transmission control protocol (TCP) packet, protocol type, etc. when packet is received key information and IP address information are read that meets the recitation of determining security association information (see column 5, lines 34-41, column 10, lines 41-50 and column 11, lines 17-45 and 40-53; column 12, lines 50-54). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Feiken et al** to determine the security association information associated for the plurality of data packets simultaneously as suggested by **Oskouy et al** because it would save time and bandwidth.

As per claims 47-48, **Feiken et al** discloses the limitation of further comprising a memory in the identification unit for storing security association information of a data packet, information belonging to the channel, key and status information (see column 4, lines 1-13 and column 5, lines 17-21) that meets the recitation of a database including security association information wherein the database is local to the classification module, and wherein the database includes one or more entries wherein each entry defines information associated with one security association.

As per claim 49, **Feiken et al** discloses the limitation of wherein the database is located on the same chip as the classification module, for example (see column 5, lines 17-21).

As per claim 55, **Feiken et al** discloses wherein the database (the organized information as disclosed in claims 47-48) is stored in memory.

As per claim 56, **Feiken et al** discloses wherein the memory is contact addressable memory (CAM) (see column 5, lines 17-21).

As per claim 57, **Feiken et al** discloses wherein the memory is random-access memory (see column 6, lines 49-52).

As per claim 60, **Feiken et al** discloses wherein the device is a network communication device (see column 3, lines 20-22).

As per claim 64, **Feiken et al** discloses a method for classifying data packets during security processing in a server (device) comprising: receiving in the device at least a portion of a header for each data packet in a plurality of data packets associated with a data flow between a source and destination (see column 3, line 65 through column 4, line 5); **Feiken et al** discloses each data packet in a plurality of data packets associated with a data flow between a source and destination (see column 1, lines 13-33); **Feiken et al** discloses determining security association information associated with each data packet in the plurality of data packets in the data flow, for

example (see column 3, line 65 through column 4, line 5); **Feiken et al** discloses receiving at least a portion of the security association information associated with a data packet in the plurality of data packets along the with the corresponding data packet at each security processing engine in a plurality of security processing engines in the device (see column 4, lines 7-25), wherein at least two of the plurality of security processing engines receive security association information for different packets in the data flow (see column 4, lines 25-41) and processing the plurality of data packets in the data flow in parallel (see column 4, lines 25-41). **Feiken et al** does not explicitly state that the classification module is configured to determine the security association information associated for the plurality of data packets simultaneously. **Oskouy et al** in an analogous art discloses receiving a plurality of data packets and performed pre-processing in parallel that meets the recitation of determining security association for the plurality of data packets simultaneously (see column 2, lines 2-5 and column 4, lines 24-29), the L3 header pre-processing that occurs in parallel includes examining the packet headers to derive a header to be stored in an associated entry in cell header queue and deriving key length, priority of the packet, whether it is a transmission control protocol (TCP) packet, protocol type, etc. when packet is received key information and IP address information are read that meets the recitation of determining security association information (see column 5, lines 34-41, column 10, lines 41-50 and column 11, lines 17-45 and 40-53; column 12, lines 50-54). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Feiken et al** to determine the security association information associated for the plurality of data packets simultaneously as suggested by **Oskouy et al** because it would save time and bandwidth.

As per claim 65, **Feiken et al** discloses the limitation of wherein the step of determining security association information comprises accessing a database to determine security association information (see column 6, lines 9-13).

As per claim 66, **Feiken et al** discloses using one or more selectors to identify a security association information entry in the database (see column 7, lines 18-25).

6. **Claims 50-54, 58, 59, 61,** and **62** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,870,479 to **Feiken et al** in view of US Patent 6,791,947 to **Oskouy et al** as applied to claims 46 and further in view of US Patent 6,484,257 to **Ellis**.

As per claim 50, **Feiken et al** substantially discloses the claimed device of claim 46. **Feiken et al** is silent about the particular information included in the header. **Ellis** in an analogous art further discloses IPSec protocol for implementing security association information which meets the recitation of wherein the security association information includes a sequence number an anti-replay window and a lifetime of the security association, one of ordinary skill in the art would recognize these properties as part of IPSec security protocol information (see **Ellis**, column 3, lines 15-64). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the device of **Feiken et al** to determine IPSec security protocol information as well known practice in the art to provide secure communications in processing data packets as suggested by **Ellis** (see column 3, lines 15-17).

As per claim 51, the references as combined above disclose the limitation of wherein the security association information further includes an encapsulating security payload (ESP) encryption algorithm identifier and one or more ESP encryption keys, for example (see **Ellis**, column 3, lines 15-64). This claim is also rejected on the same rationale as the rejection of claim 50 above.

As per claims 52-53, the references as combined above disclose the limitation of wherein the security association information further includes an (ESP) authentication algorithm identifier and one or more ESP authentication keys and an authentication header (AH) authentication algorithm identifier and one or more AH authentication keys, for example (see **Ellis**, column 3, lines 15-64). This claim is also rejected on the same rationale as the rejection of claim 50 above.

As per claim 54, **Feiken et al** discloses using security association information in the data packets to perform cryptographic operation that meets the recitation of wherein the security association information includes protocol mode information, (see column 5, lines 37-60 and column 6, lines 9-13).

As per claims 58-59 and 61, **Feiken et al** substantially discloses the claimed device of claim 46. It is obvious to one of ordinary skill in the art that the invention as combined above can be implemented in different communication device such as router, firewall, or gateway device to provide routing table computations and network management (see **Ellis**, column 8, lines 33-36 and column 9, lines 29-43 and fig. 7).

As per claim 62, **Feiken et al** substantially discloses the claimed device of claim 46 and **Ellis** further discloses wherein the device is a server (see **Ellis**, column 8, lines 58-66). This claim is also rejected on the same rationale as the rejection of claim 50 above.

7. **Claims 67-70** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,870,479 to **Feiken et al** in view of US Patent 6,791,947 to **Oskouy et al** as applied to claims 64-66 and further in view of US Patent 6,760,444 to **Leung**.

As per claim 67, **Feiken et al** substantially discloses the claimed method of claim 66. **Feiken et al** is silent about the particular selectors included in the header. **Leung** in an analogous art discloses wherein the step of determining security association information comprises accessing a database to determine security association information (see column 6, lines 13-28) and further comprises using one or more selectors to identify a security association information entry in the database wherein the one or more selectors include at least one of a destination IP address, a security protocol identifier and a security protocol identifier and a security parameter index, for example (see column 7, lines 25-37; column 3, lines 6-12). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Feiken et al** to use selectors to identify security association in the database because since a table contains one-to-many or many-to-many relationship of security information using an identifier would allow rapid retrieval of information since a secret key and other information may be associated with one identifier as suggested by **Leung**.

As per claims 68-69, the references as combined above disclose the limitation of wherein the one or more selectors include a destination IP address, a source IP address and a transport layer protocol and wherein one or more selectors further include a source port and a destination port (see **Leung**, column 7, lines 25-37 and column 9, line 52 through column 10, line 40) this is well-known in the art as included in IP header for performing IPsec processing and also disclosed in RFC 2401, "Security Architecture for IP" in Applicant's disclosure. Therefore, these claims are rejected on the same rationale as the rejection of claim 67 above.

As per claim 70, the references as combined above disclose updating or generating new security association in a database of the server to store security association information for the Home Agent that meets the recitation of wherein the step of determining security association information comprises if no security association information exists in the database associated with the packet, generating the security association information and storing the security association information in an entry in the database, for example (see **Leung**, column 7, line 50 through column 8, line 40). Therefore, this claim is rejected on the same rationale as the rejection of claim 67 above.

8. **Claim 63** is rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,870,479 to **Feiken et al** in view of US Patent 6,791,947 to **Oskouy et al** 6as applied to claims 46-62 and further in view of US Patent 6,708,273 to **Ober et al**.

As per claim 63, **Feiken et al** substantially discloses the claimed device of claim 46. **Feiken et al** does not explicitly disclose wherein the device is a network line card. **Ober et al** in an analogous art teaches a cryptographic co-processor implemented on a standard chip having encryption and hash circuits and other circuits (see column 2, lines 32-65 and column 5, lines 25-48 and abstract) within the same device for processing cryptographic operations in parallel (see column 6, lines 4-12). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the device of **Feiken et al** into a device such as a network line card because it would provide flexibility to incorporate the features of the device into any network device capable of using a network line card. The motivation to do so is also given by **Ober et al** who teaches that the plurality of encryption engines make it possible to add security to various processing applications. Hardware such as encryption and hash circuits are provided and structured to work together to provide accelerated encryption/decryption capabilities as suggested by **Ober et al** (see column 2, lines 32-65).

Conclusion

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to CARL COLIN whose telephone number is (571)272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kieu-Oanh (Krista) Bui can be reached on 571-272-7291. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Carl Colin/
Primary Examiner, Art Unit 2433
February 22, 2010